
MCSE Guide to Microsoft® Windows® 2000 Active Directory

**Will Willis
Tillman Strahan
David Watts
Barry Shilmover**

**COURSE
TECHNOLOGY**
★
THOMSON LEARNING™



MCSE Guide to Microsoft® Windows® 2000 Active Directory

by Will Willis, Tillman Strahan, David Watts, and Barry Shilmover

Managing Editor:

Stephen Solomon

Product Manager:

Charlie Blum

Associate Product Manager:

Elizabeth Wessen

Production Editor:

Catherine G. DiMassa

Text Designer:

GEX Publishing Services

Editorial Assistant:

Janet Aras

QA Manuscript Reviewer:

Nicole Ashton

Composition House:

GEX Publishing Services

COPYRIGHT © 2002 Course Technology,
a division of Thomson Learning, Inc.
Thomson Learning™ is a trademark
used herein under license.

Printed in Canada

1 2 3 4 5 6 7 8 9 TransCon 05 04 03 02 01

For more information, contact Course
Technology, 25 Thomson Place, Boston,
Massachusetts, 02210.

Or find us on the World Wide Web
at: www.course.com

ALL RIGHTS RESERVED. No part
of this work covered by the copyright
hereon may be reproduced or used in
any form or by any means—graphic,
electronic, or mechanical, including
photocopying, recording, taping, Web
distribution, or information storage and
retrieval systems—without the written
permission of the publisher.

For permission to use material from this
text or product, contact us by
Tel (800) 730-2214
Fax (800) 730-2215
www.thomsonrights.com

Disclaimer

Course Technology reserves the right to
revise this publication and make
changes from time to time in its content
without notice.

Microsoft is either a registered trade-
mark or trademark of Microsoft
Corporation in the United States and/or
other countries. Course Technology is an
independent entity from Microsoft
Corporation, and not affiliated with
Microsoft in any manner.

ISBN 0-619-01600-0

Contents

PREFACE	xvii
CHAPTER ONE	
Introduction to Active Directory	1
CHAPTER TWO	
The Structure of Active Directory	19
CHAPTER THREE	
Planning an Active Directory Implementation	43
CHAPTER FOUR	
Domain Name System (DNS)	59
CHAPTER FIVE	
Installing Active Directory	85
CHAPTER SIX	
Active Directory Configuration	115
CHAPTER SEVEN	
Administering Active Directory	151
CHAPTER EIGHT	
Performance Monitoring	175
CHAPTER NINE	
Active Directory Maintenance and Recovery	211
CHAPTER TEN	
Implementing Group Policy	233
CHAPTER ELEVEN	
Managing User Environments with Group Policy	269
CHAPTER TWELVE	
Deploying and Managing Software by Using Group Policy	301
CHAPTER THIRTEEN	
Deploying Windows 2000 Using Remote Installation Services	333
CHAPTER FOURTEEN	
Active Directory Replication	363
CHAPTER FIFTEEN	
Security	389
APPENDIX A	
Exam Objectives for MCSE Certification	413
APPENDIX B	
Hands-on Exercises	417
GLOSSARY	503
INDEX	511

TABLE OF Contents

PREFACE

xxi

CHAPTER ONE

Introduction to Active Directory

1

Windows 2000 Overview

2

The Windows 2000 Family of Operating Systems

3

The New Features in Windows 2000

4

Windows 2000 Directory Services

7

Windows 2000 and Active Directory

9

The Physical and Logical Structure of Active Directory

11

Logical Components

12

Working with Active Directory in Your Enterprise

13

Working with DNS

14

The Installation Process

14

New Overhead

15

Delegating Tasks

15

Active Directory Maintenance

15

Group Policy

16

Replication and Security Templates

16

Chapter Summary

16

CHAPTER TWO

The Structure of Active Directory

19

Active Directory Terminology

20

Domains

20

Domain Controllers

21

Trust Relationships

21

Namespace

23

Dynamic DNS

26

Domain Trees

26

Domain Forests

27

Active Directory Components	28
Active Directory Objects	28
Active Directory Schema	28
Organizational Unit	30
Global Catalog	30
Operation Masters	32
Physical Structure of Active Directory	33
Sites	33
Site Links	37
Bridgehead Servers	40
Chapter Summary	41
CHAPTER THREE	
Planning an Active Directory Implementation	43
Namespace	44
New DNS Namespace	44
Integration with an Existing Namespace	46
Site Design	47
Domain Structure	49
Uses of Organizational Units	51
Designing the Infrastructure	52
Gather Data about the Network	53
Lay Out the Active Directory Sites	53
Place the DCs within the Sites	53
Establish Replication Schedules	54
Chapter Summary	55
CHAPTER FOUR	
Domain Name System (DNS)	59
Understanding DNS Name Resolution	60
HOSTS Files and Their Function	60
Name Resolution Beyond HOSTS: DNS	60
Active Directory and DDNS	62
Forward Lookup Queries	62
Reverse Lookup Query	64

Understanding the Different Types of Name Servers	64
Primary DNS Servers	64
Secondary DNS Servers	65
Caching-Only Name Servers	65
Forwarding DNS Servers	66
Configuring and Managing DNS Zones	67
Windows 2000 Zones	68
Understanding Zone Transfers	68
Full Zone Transfer	68
Incremental Transfer	69
DNS Notify	69
Installing DNS for Active Directory	70
DNS Preinstallation	70
DNS Installation	72
Configuring DNS for Active Directory	73
Root Servers	73
Forward Lookup Zones	74
Reverse Lookup Zones	76
Resource Records	77
Dynamic DNS	80
Monitoring and Troubleshooting DNS for Active Directory	81
DNS Logging	82
nslookup	83
Chapter Summary	84
CHAPTER FIVE	
Installing Active Directory	85
Preparing for Active Directory Installation	86
Preparing IP Addressing Schemes and DNS	86
Domain Context	86
Installing Active Directory	88
Configure Your Server	88
Dcpromo.exe	89
Creating Windows 2000 Domains	90
Using the Active Directory Wizards	91
Installing the First Domain	91
Promoting a Server to a Domain Controller	101
Demoting a Domain Controller	103

Understanding the Active Directory Database	106
ntds.dit	106
Database Logging	107
Understanding Active Directory Domain Modes	108
Mixed Mode	108
Native Mode	109
Chapter Summary	112
CHAPTER SIX	
Active Directory Configuration	115
Creating a Site	116
Adding Subnets to Active Directory	118
Site Connections	120
Site Link Bridges	123
Connection Objects	125
Moving Domain Controllers between Sites	127
Global Catalog Servers	129
Operations Masters	132
Implementing Organizational Units	140
Delegating Control of Part of a Domain	141
Group Policies and OUs	147
Chapter Summary	149
CHAPTER SEVEN	
Administering Active Directory	151
Querying Active Directory	152
Common Objects	152
Finding Active Directory Objects	154
Permissions and Active Directory Objects	156
Introduction to Active Directory Permissions	156
Active Directory Security	156
Object Permissions	157
Assigning Permissions	158
Permission Inheritance	160
Making Resources Available	161
Publishing Resources	162
Publishing Network Services	162

Moving Objects	163
Moving Objects within a Domain	164
Moving Objects between Domains	164
Moving Workstations and Member Servers	167
Moving Domain Controllers between Sites	168
Moving Objects to the LostAndFound Container	168
Delegating Authority	169
Using the Delegation Of Control Wizard	171
Chapter Summary	173
CHAPTER EIGHT	
Performance Monitoring	175
Introduction to Performance Monitoring	176
Windows 2000 System Monitor	177
Memory	179
Processor	180
Disk	180
Network	180
System Monitor Terminology	181
System Monitor Data Collection	182
Objects	184
Counters	184
Instances	184
Recommended Counters	184
Counters for Memory Troubleshooting	184
Counters for Processor Troubleshooting	186
Counters for Disk Troubleshooting	187
Counters for Network Troubleshooting	188
Counters for Active Directory Troubleshooting	189
System Monitor Logging Options	191
Counter Logs	191
Trace Logs	194
Alerts	194

Event Logs	196
Application Log	196
Security Log	196
System Log	197
Directory Service	197
DNS Server	197
File Replication Service	198
Event Types	198
Viewing Remote Event Logs	199
Managing Event Logs	200
Windows Management Instrumentation	202
Tools for Monitoring Active Directory	203
LDAP Diagnostic Tool (LDPEXE)	204
Active Directory Replication Monitor (REPLMON)	204
REPADMIN	205
Chapter Summary	206

CHAPTER NINE

Active Directory Maintenance and Recovery 211

Recovery and Maintenance Overview	212
Active Directory Data Model	213
Directory System Agent (DSA)	213
The Database Layer	213
Extensible Storage Engine (ESE)	214
How Data Is Written to the Database	214
The Files of Active Directory	218
The Database File (ntds.dit)	218
The Log Files (EDB.LOG, RES1.LOG, and RES2.LOG)	218
Checkpoint Files (EDB.CHK)	219
Patch Files	219
Active Directory Dependencies	220
System State Data	220
Types of Restore	221
Non-Authoritative Restore	221
Authoritative Restore	222

Strategies for Active Directory Backup	223
Hardware Configuration of Domain Controllers	224
Active Directory Maintenance	224
Automatic Maintenance	225
Manual Database Cleanup	226
Offline Defragmentation	226
Basic Backup Principles	227
Hardware Requirements	227
Media Storage	228
Testing Restore Operations	228
Backup and Restore Security	228
The Microsoft Backup Utility	229
Chapter Summary	229

CHAPTER TEN

Implementing Group Policy 233

Understanding Group Policy Concepts	234
Windows 2000 Group Policy versus Windows NT 4 System Policies	234
Group Policy Objects	236
The Group Policy MMC Snap-in	239
Group Policy Namespace	241
Startup, Shutdown, Logon, and Logoff	246
Active Directory Structure and Group Policy	246
Group Policy Inheritance	247
Group Policy Processing	248
Group Policy Planning	250
Change Control Procedures	251
Structuring Domains and OUs for Group Policy	251
Segmented versus Monolithic GPOs	253
Cross-Domain GPO Links	253
Managing Network Bandwidth	254
Group Policy Best Practices	255
Group Policy Implementation	258
Creating a GPO	258
Creating a GPO Console	259
Specifying Group Policy Settings	262
Filtering Group Policy	263
Delegating Administrative Control of Group Policy	264
Linking a GPO	266
Chapter Summary	266

CHAPTER ELEVEN**Managing User Environments with Group Policy 269**

Using Scripts to Apply Configuration Settings to Users and Computers	270
Overview of Scripts	270
Windows Scripting Host	271
Assigning Scripts through Group Policy	275
Controlling the User Environment through Administrative Templates	279
ADM Files	280
Computer Templates	287
User Templates	290
Using Folder Redirection to Move User Files to a Server	294
Folder Redirection Notes	297
Advantages of Folder Redirection	298
Chapter Summary	298

CHAPTER TWELVE**Deploying and Managing Software by Using Group Policy 301**

IntelliMirror Components and Change and Configuration Management Concepts	302
Hard versus Soft Costs	302
IntelliMirror	303
Understanding the Phases of Software Management	305
Preparation Phase	306
Distribution Phase	307
Targeting Phase	308
Pilot Phase	308
Installation Phase	310
Creating and Configuring Windows Installer Packages	310
Windows Installer Technology Overview	311
Managing Windows Installer Settings with Group Policy	312
Creating Windows Installer Packages with Win INSTALL LE	314
Managing Software Deployment through the Software Installation Snap-in	321
Requirements for Software Installation	321
Assigned versus Published Applications	323
Using the Software Installation Snap-in	323
Patching Software Using the Windows Installer Package Editor	329
Patching Applications	331
Chapter Summary	331

CHAPTER THIRTEEN**Deploying Windows 2000 Using Remote Installation Services 333**

RIS Overview	334
How RIS Functions	335
RIS Requirements	335
Remote Installation Services	335
Domain Name System (DNS)	336
Dynamic Host Configuration Protocol (DHCP) Server	336
Active Directory	336
RIS Client and Server Components	336
Client Requirements of RIS	337
Server Components of RIS	339
Setting Up and Configuring RIS	340
RISetup	342
Creating RIS Images	347
RIPrep	347
Creating Images with RIPrep	348
Creating RIS Boot Disks	354
Managing RIS Security	355
Authorizing an RIS Server	355
Managing RIS Client Options with Group Policy	356
Managing RIS Configuration Settings	357
Chapter Summary	361

CHAPTER FOURTEEN**Active Directory Replication 363**

Introduction to Active Directory Replication	364
Elements of Active Directory Replication	365
The Replication Process Illustrated	372
Replication Conflicts Illustrated	380
Intersite and Intrasite Replication	386
Chapter Summary	387

CHAPTER FIFTEEN	
Security	389
What Is Auditing?	391
Planning Your Audit Policy	392
Local Policies and Domain Policies	394
Configuring Group Policy	395
Auditing Files and Folders	398
Auditing Active Directory Objects	400
Auditing Printers	401
Tips for Auditing	401
Security Templates	402
Preconfigured Security Templates	402
Viewing Security Templates Configurations	405
Using Security Templates with GPOs	407
The Security Configuration and Analysis Tool	409
Chapter Summary	411
 APPENDIX A	
Exam Objectives for MCSE Certification	413
 APPENDIX B	
Hands-on Exercises	417
 GLOSSARY	503
 INDEX	511

Preface

Welcome to the *MCSE Guide to Microsoft Windows 2000 Active Directory*! This book provides in-depth coverage of the knowledge and skills required to pass Microsoft certification exam #70-217: *Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure*. This course of study prepares a network professional to work in medium to very large computing environments that use the Windows 2000 network operating system. Organizations place greater and greater demand on their networks and the services those networks deliver, often providing round-the-clock services to both internal and external clients. Therefore, there is increased demand for network professionals who can design flexible, usable directory service implementations that can properly advertise and support all necessary network services, as well as the users and groups who make use of them.

THE INTENDED AUDIENCE

The goal of this book is to teach directory services implementation and administration to individuals who desire to learn about that topic for practical purposes, as well as those who wish to pass Microsoft certification exam #70-217. This book provides the content for all the skills measured on that exam, but also provides related information that is not directly tested.

Chapter 1, “Introduction to Active Directory,” provides an overview of the concepts and capabilities inherent in Microsoft’s Active Directory directory services environment, so essential to the proper design and delivery of network services on large, complex networks. Chapter 1 explains the logical and physical structures of Active Directory, and introduces the basics involved in working with Active Directory from initial directory design, through the installation process, and in working with and maintaining Active Directory thereafter. **Chapter 2**, “The Structure of Active Directory,” explores the server roles involved in operating an Active Directory environment, the various components that appear within Active Directory databases, and the physical structures into which Active Directory installations fall. **Chapter 3**, “Planning an Active Directory Implementation,” focuses on understanding an organization’s physical and political structures and explains how to map them into appropriate namespaces, site designs, domain structures, and organizational units (OUs).

Chapter 4, “Domain Name System (DNS),” explores the structures, functions, and relationships among name servers, and how those servers interact to maintain an up-to-date distributed DNS database. Chapter 4 also explores how to integrate and manage DNS alongside Active Directory, particularly to support a Dynamic DNS (DDNS) environment.

Chapter 5, “Installing Active Directory,” zeroes in on preparations for and installation of Active Directory, including domain creation and working with Active Directory Wizards. Chapter 5 also explains how to properly understand the Active Directory database and Active Directory domain modes.

Chapter 6, “Active Directory Configuration,” picks up where Chapter 5 leaves off, as it describes the requirements for and activities involved in configuring Active Directory for any specific installation. Chapter 6 covers all the necessary details involved in site creation and in implementing organizational units and using them to delegate authority and manage groups.

Chapter 7, “Administering Active Directory,” focuses on the ongoing maintenance and upkeep involved in managing an Active Directory environment, including how to query the database, working with permissions, managing resources, moving objects around a directory tree or forest, and delegating authority.

Chapter 8, “Performance Monitoring,” begins with a basic overview of Windows 2000 performance monitoring terms, tools, and techniques. Chapter 8 continues with coverage of the Windows 2000 System Monitor, along with objects and counters relevant to Active Directory, as well as event logs, specific instrumentation, and tools specific to monitoring Active Directory per se. **Chapter 9**, “Active Directory Maintenance and Recovery,” looks at what’s involved in protecting the Active Directory database, and in recovering from errors or failures that affect this vital service. Topics covered include a review of the Active Directory Data model, discussion of key Active Directory files and dependencies, plus issues related to backing up, cleaning up, and restoring Active Directory itself.

Chapter 10, “Implementing Group Policy,” covers key concepts related to the Group Policy Object, and explains how to plan and implement effective Group Policies. **Chapter 11**, “Managing User Environments with Group Policy,” picks up where Chapter 10 leaves off, as it explores how to use scripts and administrative templates to control the user environment, and how to use folder redirection to relocate user files on some server. **Chapter 12**, “Deploying and Managing Software by Using Group Policy,” explores further use of the Group Policy Object, along with system components like IntelliMirror, to prepare, distribute, and manage software deployment in an Active Directory based environment.

Chapter 13, “Deploying Windows 2000 Using Remote Installation Services,” explores what RIS can do, and how it works with DNS, DHCP, and Active Directory to enable easy remote installation of Windows 2000 clients and servers. **Chapter 14**, “Active Directory Replication,” explores the replication process in an Active Directory environment, including its intra- and inter-site behavior. **Chapter 15**, “Security,” addresses security matters relevant

to Active Directory, including auditing, security templates, and the Security Configuration and Analysis Tool.

FEATURES

To ensure a successful learning experience, this book includes the following pedagogical features:

- **Chapter Objectives:** Each chapter in this book begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with a quick reference to the contents of that chapter, as well as a useful study aid.
- **Illustrations and Tables:** Numerous illustrations of server screens and components aid you in the visualization of common setup steps, theories, and concepts. In addition, many tables provide details and comparisons of both practical and theoretical information and can be used for a quick review of topics.

At the end of each chapter is a Chapter Summary, a bulleted list is that gives a brief but complete summary of the chapter.

Appendix B includes the following features to reinforce the material covered in each chapter:

- **Key Terms List:** A list of all new terms and their definitions for each chapter.
- **Review Questions:** A list of review questions tests your knowledge of the most important concepts covered in each chapter.
- **Hands-on Projects:** Hands-on projects help you to apply the knowledge gained in each chapter.
- **Case Projects:** Case projects take you through real-world scenarios for the material covered in each chapter.

On the CD-ROM: On the CD-ROM you will find **CoursePrep**[®] exam preparation software, which provides 50 sample MCSE exam questions mirroring the look and feel of the MCSE exams, and **CourseSim**[®] simulation software, which allows you to perform tasks in a simulated Active Directory environment.

TEXT AND GRAPHIC CONVENTIONS

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are as follows:



The Note icon is used to present additional helpful material related to the subject being described.



Each Hands-on Project in this book is preceded by the Hands-On icon and a description of the exercise that follows.



Case project icons mark the case project. These are more involved, scenario-based assignments. In this extensive case example, you are asked to implement independently what you have learned.

INSTRUCTOR'S MATERIALS

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM.

Electronic Instructor's Manual. The Instructor's Manual that accompanies this textbook includes:

- Additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
- Solutions to all end-of-chapter materials, including the Review Questions, Hands-on Projects, and Case Projects.

ExamView® This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

PowerPoint presentations. This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Read This Before You Begin

TO THE USER

This book was written with the network professional in mind. It provides an excellent preparation for the Microsoft certification exam #70-217, and also for the real-life tasks involved in implementing and administering directory services for today's networks, which must support an ever-increasing variety of users, services, and applications. To fully benefit from the content and the projects presented here, you will need access to a classroom lab containing computers configured as follows:

- **Windows 2000 Server or Windows 2000 Advanced Server.** In a classroom lab situation each student or pair of students should have a computer capable of running Windows 2000 Server or Windows 2000 Advanced Server.
- An Internet connection is helpful, and will be required for some of the case projects.

VISIT OUR WORLD WIDE WEB SITE

Additional materials designed especially for you might be available for your course on the World Wide Web. Go to *www.course.com*. Search for this book title periodically on the Course Technology Web site for more details.

TO THE INSTRUCTOR

When setting up a classroom lab, make sure each student workstation is capable of running Windows 2000 Server. Students will need access to the Windows 2000 source files when they install Windows 2000 Server and when they require access to various services during the hands-on projects. Detailed setup instructions for the labs are contained in the Instructor's Manual.
